IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

AMERICAN HOSPITAL ASSOCIATION, et al., Plaintiffs, v. XAVIER BECERRA, et al., Defendants,	Case No. 23-CV-1110-P

DEFENDANTS' COMBINED BRIEF IN OPPOSITION TO PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF DEFENDANTS' CROSS-MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

INTRODUCTION 1

STATUTORY AND REGULATORY BACKGROUND 5

I. HIPAA AND THE HIPAA RULES 5

II. THE BULLETIN 9

PROCEDURAL HISTORY 14

LEGAL STANDARD 14

ARGUMENT 15

I. THE COURT LACKS JURISDICTION OVER PLAINTIFFS' CLAIMS. 15

A. The Revised Bulletin Is Not Final Agency Action. 15

B. Plaintiffs Cannot Avoid the Finality Requirement by Recasting a Garden-Variety APA Claim as a Non-statutory Equitable Claim. 21

II. PLAINTIFFS' CLAIMS FAIL ON THE MERITS. 27

A. The Revised Bulletin Is Consistent with HIPAA's Definition of IIHI. 27

B. The Revised Bulletin Is Not Arbitrary and Capricious. 38

C. The Revised Bulletin Did Not Require Notice-and-Comment Procedures. 41

III. ANY RELIEF SHOULD BE APPROPRIATELY TAILORED. 44

CONCLUSION 45

TABLE OF AUTHORITIES

CASES

Ala. Rural Fire Ins. Co. v. Naylor,
530 F.2d 1221 (5th Cir. 1976) 22

Alaska Dep't of Env't Conservation v. EPA,
540 U.S. 461 (2004) 38

Am. Acad. of Implant Dentistry v. Parker,
860 F.3d 300 (5th Cir. 2017) 37

Am. Airlines Inc. v. Hermann,
176 F.3d 283 (5th Cir. 1999) 23, 24

Amin v. Mayorkas,
24 F.4th 383 (5th Cir. 2022) 14

Apter v. HHS,
80 F.4th 579 (5th Cir. 2023) 22, 23, 25, 26

Armstrong v. Exceptional Child Ctr., Inc.,
575 U.S. 320 (2015). 22

AT&T Co. v. EEOC,
270 F.3d 973 (D.C. Cir. 2001) 18

Bd. of Governors. of Fed. Rsrv. Sys v. MCorp Fin., Inc.,
502 U.S. 32 (1991) 24

Bd. of Trs. of State Univ. of N.Y. v. Fox,
492 U.S. 469 (1989) 37

Beiser v. Weyler,
284 F.3d 665 (5th Cir. 2002) 27

Bennett v. Spear,
520 U.S. 154 (1997) 15

Block v. N. Dakota ex rel. Bd. of Univ. & Sch. Lands,
461 U.S. 273 (1983) 25

Bluefield Water Ass'n, Inc. v. City of Starkville, Miss.,
577 F.3d 250 (5th Cir. 2009) 44

Boelter v. Advance Mag. Publ'rs Inc.,
210 F. Supp. 3d 579 (S.D.N.Y. 2016) 36

Boelter v. Hearst Commc'ns Inc.,
192 F. Supp. 3d 427 (S.D.N.Y. 2016) 36, 37

Braidwood Mgmt., Inc. v. EEOC,
70 F.4th 914 (5th Cir. 2023) 26

Brown Exp., Inc. v. United States,
607 F.2d 695 (5th Cir. 1979) 42

Central Hudson Gas & Electric Corp. v. Public Service Commission of New York,
447 U.S. 557 (1980) 36

Chrysler Corp. v. Brown,
441 U.S. 281 (1979) 41

Consumer Elecs. Ass'n v. FCC,
347 F.3d 291 (D.C. Cir. 2003) 40

Cousin v. Sharp Healthcare,
No. 22-cv-2040, 2023 WL 8007350 (S.D. Cal. Nov. 17, 2023) 29, 34

Danos v. Jones,
652 F.3d 577 (5th Cir. 2011) 22, 23, 24

Data Mktg. P'ship v. U.S. Dep't of Labor,
45 F.4th 846 (5th Cir. 2022) 45

Dobbs v. Jackson Women's Health Organization,
597 U.S. 215 (2022) 19

eBay Inc. v. MercExchange, L.L.C.,
547 U.S. 388 (2006) 44

Exxon Chems. Am. v. Chao,
298 F.3d 464 (5th Cir. 2002) 17, 24

FCC v. ITT World Commc'ns, Inc.,
466 U.S. 463 (1984) 25

FCC v. Prometheus Radio Project,
592 U.S. 414 (2021) 38, 39

Fed. Exp. Corp. v. U.S. Dep't of, Comm.,
39 F.4th 756 (D.C. Cir. 2022) 22, 23, 24

Flight Training Int'l, Inc. v. FAA,
58 F.4th 234 (5th Cir. 2023) 41, 42

Geyen v. Marsh,
775 F.2d 1303 (5th Cir. 1985) 22

Griffith v. Fed. Labor Rel. Auth.,
842 F.2d 487 (D.C. Cir. 1988) 23

Harris Cnty. v. MERSCORP Inc.,
791 F.3d 545 (5th Cir. 2015) 26

Hartley v. Univ. of Chi. Med. Ctr.,
No. 22 C 5891, 2023 WL 7386060 (N.D. Ill. Nov. 8, 2023) 34

In re Meta Pixel Healthcare Litig.,
647 F. Supp. 3d 778 (N.D. Cal. 2022) 28

Jafarzadeh v. Duke,
270 F. Supp. 3d 296 (D.D.C. 2017) 25

Kurowski v. Rush Sys. for Health,
No. 22 C 5380, 2023 WL 4707184 (N.D. Ill. July 24, 2023) 34

Leedom v. Kyne,
358 U.S. 184 (1958) 24

Lincoln v. Vigil,
508 U.S. 182 (1993) 41

Louisiana v. U.S. Army Corps of Eng'rs,
834 F.3d 574 (5th Cir. 2016) 15, 16

Lujan v. Nat'l Wildlife Fed'n,
497 U.S. 871 (1990) 15

Luminant Generation Co. v. U.S. EPA,
757 F.3d 439 (5th Cir. 2014) 18

Medina Cnty. Env't Action Ass'n v. Surface Transp. Bd.,
602 F.3d 687 (5th Cir. 2010) 38

Mendoza v. Perez,
754 F.3d 1002 (D.C. Cir. 2014) 42

Michigan v. EPA,
576 U.S. 743 (2015) 39

Mock v. Garland,
75 F.4th 563 (5th Cir. 2023) 43

Monsanto Co. v. Geertson Seed Farms,
561 U.S. 139 (2010) 44

Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,
463 U.S. 29 (1983) 38

Nat'l Ass'n of Mfrs. v. SEC,
748 F.3d 359 (D.C. Cir. 2014) 40

Nat'l Fed'n of Indep. Bus. v. Dougherty,
No. 3:16-CV-2568, 2017 WL 1194666 (N.D. Tex. Feb. 3, 2017) 20

Nat'l Pork Producers Council v. U.S. EPA,
635 F.3d 738 (5th Cir. 2011) 15

Neb. State Legis. Bd. United Transp. Union v. Slater,
245 F.3d 656 (8th Cir. 2001) 24

Nyunt v. Chairman, Broadcasting Bd. of Governors,
589 F.3d 445 (D.C. Cir. 2009) 22, 24

Oestereich v. Selective Serv. Sys. Loc. Bd. No. 11,
393 U.S. 233 (1968) 23

Pennhurst State Sch. & Hosp. v. Halderman,
465 U.S. 89 (1984) 23

Peoples Nat'l Bank v. Off. of Comptroller of Currency of the U.S.,
362 F.3d 333 (5th Cir. 2004) 16

Perez v. Mortg. Bankers Ass'n,
575 U.S. 92 (2015) 41, 42

POET Biorefining, LLC v. EPA,
970 F.3d 392 (D.C. Cir. 2020) 42

Prof'ls & Patients for Customized Care v. Shalala,
56 F.3d 592 (5th Cir. 1995) 19

Puerto Rico v. United States,
490 F.3d 50 (1st Cir. 2007) 24

Qureshi v. Holder,
663 F.3d 778 (5th Cir. 2011) 15

Rhea Lana, Inc. v. Dep't of Labor,
824 F.3d 1023 (D.C. Cir. 2016) 15

Ryder Truck lines, Inc. v. United States,
716 F.2d 1369 (11th Cir. 1983) 19

S.C. Med. Ass'n v. Thompson,
327 F.3d 346 (4th Cir. 2003) 5

Shalala v. Guernsey Mem'l Hosp.,
514 U.S. 87 (1995) 42

Sierra Club v. U.S. Dep't of Interior,
990 F.3d 909 (5th Cir. 2021) 38

Skelly Oil Co. v. Phillips Petroleum Co.,
339 U.S. 667 (1950) 26

Smith v. Facebook, Inc.,
745 F. App'x 8 (9th Cir. 2018) 34

Sorrell v. IMS Health Inc.,
564 U.S. 552 (2011) 35, 38

Spring Branch Wildlife Preserve v. U.S. EPA,
No. 3:20-cv-225, 2021 WL 6503917 (S.D. Tex. Sept. 17, 2021) 17

Texas v. Becerra,
89 F.4th 529 (5th Cir. 2024) 19, 20

Texas v. Brooks-LaSure,
No. 6:23-cv-161, 2023 WL 4304749 (E.D. Tex. June 30, 2023) 20

Texas v. EEOC,
933 F.3d 433 (5th Cir. 2019) 20

Texas v. HHS,
No. 23-cv-22, --- F. Supp. 3d ----, 2023 WL 4629168 (W.D. Tex. July 12, 2023) 20

Texas v. United States,
809 F.3d 134 (5th Cir. 2015) 41

Trans Union Corp. v. FTC,
245 F.3d 809 (D.C. Cir. 2001) 37

U.S. West, Inc. v. FCC,
182 F.3d 1224 (10th Cir. 1999) 36

United States v. Oakland Cannabis Buyers' Co-op.,
532 U.S. 483 (2001) 35

United States v. Texas,
143 S. Ct. 1964 (2023) 45

Webster v. Fall,
266 U.S. 507 (1925) 26

Younger v. Harris,
401 U.S. 37 (1971) 25

STATUTES

5 U.S.C. § 553(b)(A) 41

5 U.S.C. § 704 15

5 U.S.C. § 706(2)(C) 22, 24

42 U.S.C. § 1320d-1(a) 6

42 U.S.C. § 1320d-2 5

42 U.S.C. § 1320d-5 ..... 8, 9

42 U.S.C. § 1320d(6) 1, 4, 7, 27

Pub. L. No. 104-191, § 264 5

FEDERAL RULE

Fed. R. Civ. P. 56(a) 14

ADMINISTRATIVE AND EXECUTIVE MATERIALS

45 C.F.R. part 160 44

45 C.F.R. § 160.101 6

45 C.F.R. § 160.103 ..... *passim*

45 C.F.R. § 160.548(a) 9

45 C.F.R. § 164.102 ..... 6, 8

45 C.F.R. § 164.502 ..... *passim*

45 C.F.R. § 164.508 13

45 C.F.R. § 164.514 ..... 7, 17, 29, 35

45 C.F.R. §§ 160.306, 160.308, 160.312, 160.314, 160.402 9

45 C.F.R. §§ 160.420(b), 160.504, ... 9

45 C.F.R. §§ 164.400–414 8

Standards for Privacy of Individually Identifiable Health Information,
65 Fed. Reg. 82,462 (Dec. 28, 2000)
(codified at 45 C.F.R. § 160.101, *et seq.* and 45 C.F.R. § 164.102, *et seq.*) ..... *passim*

Factoring Criteria for Firearms with Attached "Stabilizing Braces,"
88 Fed. Reg. 6478, 6481 (Jan. 31, 2023) 44

OTHER AUTHORITIES

Black's Law Dictionary (11th ed. 2019)
(defining "related") 27

Merriam-Webster's Dictionary
(defining "relate"), https://www.merriam-webster.com/dictionary/relate%20to. 27

33 Charles A. Wright & Arthur R. Miller,
Fed. Prac. & Proc. § 8307 (3d ed. Apr. 2020 update)..... 25

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations (the HIPAA Privacy, Security, and Breach Notification Rules or HIPAA Rules) ensure that Americans can seek health care without fearing that their sensitive health information will be made public. Recognizing the harms that result from the disclosure of health information and the deleterious effect that inadequate privacy protections can have on the health care system, HIPAA's regulations have long prohibited covered entities, including certain health care providers, from disclosing individually identifiable health information (IIHI) to third parties except as expressly permitted by the regulations or authorized by the individual. In delineating the types of information that must be protected, Congress chose to sweep broadly, instructing that entities covered by HIPAA must protect "any information" that (1) "relates to" the past, present, or future health condition, health care, or payment of health care of any individual, (2) as to which there is a reasonable basis to believe that the information can be used to identify the individual. 42 U.S.C. § 1320d(6).

Notwithstanding these serious privacy concerns, many HIPAA covered entities disclose copious amounts of information to third parties through online tracking technologies. A tracking technology is a computer code or script embedded in a webpage that harvests data about users who navigate to and interact with the webpage. Such technologies capture information like the title and contents of the webpage visited, users' interactions on a website—including what information they enter or click on while there and what links or search terms brought them there—along with information about the user, like email or IP addresses. They then share that information with outside companies for uses ranging from website analytics and usability testing to creating user profiles and targeted advertising. When used on the websites of HIPAA covered entities, these

technologies (depending on the particular webpage and technology used) can gather and disclose information that can be used to identify an individual and show, for example, that individual attempted to schedule an appointment with a particular provider, identified symptoms from which they are currently suffering, or searched for information about their specific medical conditions or potential treatment options.

Some HIPAA covered entities have recognized the privacy risks inherent in the use of tracking technologies—indeed, before the release of the guidance at issue here, some covered entities reported such disclosures as breaches of unsecured protected health information under the HIPAA Breach Notification Rule to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS). OCR also came to understand, however, that many entities may have failed to consider applying HIPAA's privacy standards to protected health information (PHI) disclosed to third parties through tracking technologies. In light of the risk that sensitive health information could be disclosed to third parties through these technologies, in December 2022 OCR issued a guidance document—the Bulletin challenged in Plaintiffs' complaint—reminding HIPAA covered entities and business associates that the HIPAA Privacy Rule's longstanding restrictions on disclosing PHI applies to information gathered and disclosed through online tracking technologies. *See* U.S. Dep't of Health & Human Servs., *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, AR18-31.[1] The original Bulletin reminded regulated entities that they must comply with HIPAA's regulatory requirements when using those technologies. And it reminded entities that the HIPAA Rules permit the use of online tracking technologies when implemented properly by, for example, entering into contracts with vendors who agree to safeguard the privacy and security of IIHI or by

[1] Citations to "AR" refer to pages in the certified administrative record. *See* ECF No. 49.

obtaining HIPAA authorizations from individuals. In March 2024, OCR replaced the original Bulletin with a revised version—the Revised Bulletin—designed to provide additional clarity to regulated entities and the public about what types of disclosures to tracking technologies might reveal IIHI, to offer additional advice about ways regulated entities can use tracking technologies and also comply with the Privacy Rule, and to share OCR's enforcement priorities in investigations concerning disclosures to tracking technologies. AR1–17. Although the Revised Bulletin superseded the original Bulletin, Defendants' understanding is that Plaintiffs do not believe the Revised Bulletin resolves their claims.[2]

Plaintiffs challenge a narrow portion of the Revised Bulletin—specifically, its application to the use of tracking technologies on certain "unauthenticated" webpages (i.e., pages that neither require nor request a user to input a username, password, or other log-in credential before accessing the page). They contend that information gathered from unauthenticated websites can never satisfy HIPAA's definition of IIHI. Plaintiffs also argue that the Revised Bulletin is arbitrary and capricious and was improperly issued without notice and comment. Each of these claims fails.

As a threshold matter, the Court lacks jurisdiction over Plaintiffs' claims. Judicial review under the Administrative Procedure Act (APA) is reserved for final agency action, which the Revised Bulletin is not. The Revised Bulletin neither reflects the agency's position on any particular case nor imposes any new legal obligations over and above what are already required by HIPAA's regulations—indeed, it expressly states that it is "not meant to bind the public in any way" but intended "only to provide clarity to the public regarding existing requirements." AR11.

[2] Plaintiffs' opening brief, filed before the Revised Bulletin was issued, discusses only the original Bulletin. Because the original Bulletin has been superseded, it can no longer be set aside or enjoined, as Plaintiffs originally requested. *See* Compl. at 21. Accordingly, this brief generally addresses the Revised Bulletin.

Indeed, the Revised Bulletin is simply a reminder of the applicability of the HIPAA Rules to disclosures of protected health information online, issued in response to information OCR received suggesting that some regulated entities were not following the Rules.

Even if the Court had jurisdiction, Plaintiffs' claims fail on the merits. Plaintiffs argue that the Revised Bulletin conflicts with HIPAA because information collected by online tracking technologies on unauthenticated webpages cannot constitute IIHI. But there is no such conflict. As the Revised Bulletin makes plain, whether web trackers used on unauthenticated webpages might result in disclosures of PHI is a fact-specific question that turns upon whether the information collected relates to an identifiable individual's past, present, or future health, health care, or payment for health care. AR5–7. This guidance is entirely consistent with HIPAA and the HIPAA Rules. As the Revised Bulletin explains, a tracking technology that collects identifying information—such as an IP address—from an individual who, say, uses a hospital's website to book an appointment with a psychiatrist or enters information about their own psychiatric condition into an online symptom checker may have collected information that both "relates to" the individual's health care and that "reasonabl[y]" can be used to identify the individual. 42 U.S.C. § 1320d(6); *see also* AR5–7. Conversely, a tracking technology that collects identifying information from an individual visiting a website showing a hospital's job postings or looking into services the hospital provides for the purpose of researching a school paper likely would not have collected IIHI because the website visits appear to be unrelated to the individual's health or health care. AR5–7. Thus, the Revised Bulletin makes clear that its guidance as to when IIHI is likely disclosed to tracking technologies aligns with the statutory and regulatory text.

In addition, Plaintiffs cannot show that the agency acted unreasonably in issuing the Revised Bulletin. The Revised Bulletin sufficiently explains OCR's understanding of how

HIPAA's regulations apply to IIHI, and that understanding is consistent with HIPAA's statutory language and the balance struck in its regulations between the benefits of electronic health information and the harms to individuals and society resulting from inadequate privacy protections. Finally, the APA exempts non-binding guidance documents like the Revised Bulletin from notice-and-comment rulemaking procedures.

For these reasons, as explained further below, the Court should deny Plaintiffs' motion for summary judgment and grant Defendants' cross-motion for summary judgment.

STATUTORY AND REGULATORY BACKGROUND

I. HIPAA AND THE HIPAA RULES

Congress enacted HIPAA in 1996 in response to the growing use of electronic information systems in health care. HIPAA directed the Secretary of HHS to adopt uniform national standards "to enable health information to be exchanged electronically" in order "to improve the . . . efficiency and effectiveness of the health care system." Pub. L. No. 104-191, §§ 261-62, 110 Stat. 936 (1996); 42 U.S.C. § 1320d-2. However, in light of the "paramount" need to protect the privacy of Americans' sensitive health information, H.R. Rep. No. 104-496, at 100 (1996), Congress also tasked the Secretary with promulgating standards to ensure the privacy of IIHI. *See* Pub. L. No. 104-191, § 264.

As directed by HIPAA, the Secretary submitted to Congress "detailed recommendations" on privacy standards for IIHI, *id.* § 264(a), and with Congress's acquiescence, "promulgate[d] final regulations containing such standards," *id.* § 264(c)(1), in the 2000 "Privacy Rule." *See generally S.C. Med. Ass'n v. Thompson*, 327 F.3d 346, 348 (4th Cir. 2003); *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. § 160.101, *et seq.* and 45 C.F.R. § 164.102, *et seq.*). The Privacy Rule was intended to

respond to the public's significant concerns about the lack of privacy of individuals' health information and the harms that result from a loss of privacy. 65 Fed. Reg. at 82,464–65. As HHS explained, "[t]he provision of high-quality health care requires the exchange of personal, often-sensitive information," and individuals' trust that their information will be kept confidential is essential to the efficient and effective operation of the nation's health care system. *Id.* at 82,463. Moreover, the harms suffered by individuals when their sensitive health information is revealed—including unwanted intrusion, identity theft, and embarrassment—are severe, and the public's fear of those harms impedes the provision of health care. *Id.* at 82,464–65. At the same time, while the electronic transmission of health information "affords many benefits to individuals and to the health care industry," *id.* at 82,465, the market incentives for health care plans and providers "discourage privacy protection," *id.* at 82,761. Health care plans and providers "gain[] the full benefit of using such information" but the individual "suffer[s] the losses from disclosure," encouraging the "over-use" of IIHI. *Id.* at 82,761–62. The Privacy Rule thus "seeks to balance the needs of the individual with the needs of the society," *id.* at 82,464, by requiring entities covered by HIPAA to protect sensitive health information while allowing certain limited disclosures "to improve the efficiency and effectiveness of health care delivery," *id.* at 82,463.

To that end, the Privacy Rule restricts the use and disclosure of PHI by "covered entities" and their "business associates." 45 C.F.R. § 164.502. Generally speaking, a covered entity is a health care plan, health care provider, or health care clearinghouse that transmits "any health information in electronic form in connection with a transaction covered by" HIPAA. *Id.* § 160.103; *see also* 42 U.S.C. § 1320d-1(a). PHI is defined as IIHI transmitted or maintained in electronic media or in any other form or medium (with exceptions not relevant here), 45 C.F.R. § 160.103, and IIHI is defined by both HIPAA and the Privacy Rule as any information that (1) "is created or

received by" a covered entity; (2) "relates to" either "the past, present, or future physical or mental health or condition of an individual"; the "provision of health care to an individual"; or the "past, present, or future payment for the provision of health care to an individual"; and (3) either "identifies the individual" or "with respect to which there is a reasonable basis to believe that the information can be used to identify the individual," 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103 (same).[3]

The Privacy Rule further enumerates specific categories of information that constitute individual "identifiers." 45 C.F.R. § 164.514(b)(2)(i) (specifying "identifiers" that must be removed from PHI for it to be considered de-identified). These identifiers have always included not just information like names, social security numbers, and account numbers, but also geographic locations, email addresses, IP addresses, and "[a]ny other unique identifying number, characteristic, or code." *Id.* § 164.514(b)(2)(R).

A covered entity is not permitted to "use or disclose" PHI except as specifically authorized by the Privacy Rule. *Id.* § 164.502(a). The Privacy Rule identifies several permissible and mandatory uses and disclosures, including, *inter alia*, disclosures for the provision of or payment for health care; for "health care operations"; in connection with judicial or administrative proceedings; and for research purposes. *See id.* §§ 164.502(a)(1)–(2), 164.512. Covered entities are also permitted to disclose PHI to a "business associate," *id.* § 164.502(a)(3), which is generally an entity that operates on behalf of a covered entity for certain functions involving the creation, transmission, receipt, or maintenance of PHI, including administration, data analysis, and practice management, or provides certain services to a covered entity, such as consulting or administrative

[3] The term "PHI" under the HIPAA Rules largely incorporates the definition of IIHI under HIPAA. *See* 45 C.F.R. § 160.103.

services, that involve the disclosure of PHI, *id.* § 160.103. A business associate relationship must be subject to a contract or other written arrangement (known as a "business associate agreement") that outlines the authorized uses and disclosures of PHI and requires the business associate to use appropriate safeguards to protect the privacy of individuals' PHI. *Id.* §§ 164.502(e)(1), 164.504(e)(1). Except for certain prohibited uses, covered entities may also disclose PHI pursuant to a valid authorization from the individual. *Id.* § 164.502(a)(1)(iv). In general, when using or disclosing PHI for permitted purposes, covered entities "must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose." *Id.* § 164.502(b)(1).

Covered entities and business associates (collectively, "regulated entities") are also subject to the HIPAA Security and Breach Notification Rules. The Security Rule requires regulated entities to maintain reasonable and appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic PHI; to protect against any reasonably anticipated threats or hazards to the security of electronic PHI; and to protect against reasonably anticipated impermissible uses or disclosures. 45 C.F.R. §§ 164.102–106, 164.302–318. The Breach Notification Rule requires regulated entities to provide notification of a breach of unsecured PHI to the Secretary of HHS; to affected individuals to alert them that their PHI has been compromised and to encourage them to take the necessary steps to prevent any resulting harm; and, in situations in which a breach affects more than 500 residents of a state or jurisdiction, to a prominent media outlet serving that state or jurisdiction. 45 C.F.R. §§ 164.400–414.

Violations of the HIPAA Privacy, Security, and Breach Notification Rules are civilly enforced by OCR. OCR is authorized to investigate regulated entities, and if it finds a violation, may informally resolve the matter with the entity through compliance or corrective measures or seek to impose monetary penalties. *See* 42 U.S.C. § 1320d-5; 45 C.F.R. §§ 160.306, 160.308,

160.312, 160.314, 160.402. If OCR seeks to impose a monetary penalty on an entity, the entity may request an administrative hearing before an administrative law judge, 45 C.F.R. §§ 160.420(b), 160.504, and appeal any adverse decision to a board of administrative law judges, 45 C.F.R. § 160.548(a). The board's decision is subject to judicial review in a federal court of appeals. 42 U.S.C. § 1320d-5 (incorporating provisions of 42 U.S.C. § 1320a-7a); *id.* § 1320a-7a(e).

II. THE BULLETIN

On December 1, 2022, OCR issued the original Bulletin to "highlight" and remind regulated entities how their obligations under the HIPAA Rules continue to apply to PHI when they use online tracking technologies. AR18-31. Online tracking technologies are computer scripts or codes embedded in a website or mobile application that gather and share information collected from users as they interact with particular webpages, sometimes even after they navigate away from the original website. AR19–20. The data collected by tracking technologies differ depending on the particular tracking technology employed, but tracking technologies generally collect information about the webpage visited—such as its URL, its title, its full contents, the search terms used by the user to reach the page, and what buttons the user clicked on the page or the path that led them to the page—and can link that with identifying information about users, such as email addresses, IP addresses, geographical locations, and medical record numbers. AR231–37. User data can be logged across multiple visits, and certain tracking technologies are also capable of linking data collected from users with their other accounts, such as Google or Facebook accounts. AR228–29; AR231–32.

Tracking technologies are a pervasive feature of the Internet and are used by website operators and third-party technology vendors, like Meta and Google, to glean information about

users and their online activities for various reasons, including website analytics and targeted advertising. AR227–28. Regulated entities frequently engage third-party vendors to deploy tracking technologies on their websites. AR227, AR234–37. In such circumstances, the tracking technology functions by sending information collected on the regulated entity's website directly to the third-party vendor. AR3, AR228. The information is generally not de-identified prior to its transmission. AR228–37. Though some tracking technology vendors may represent that they do not further disclose identifying information collected from regulated entities' websites, *see* Br. of Amici Curiae Thirty Hosps. and Hosp. Sys. In Supp. of Pls.' Mot. for Summ. J. at 15, ECF No. 35, a regulated entity may not make an initial disclosure of PHI to a tracking technology vendor unless the Privacy Rule expressly permits the disclosure and any applicable conditions have been met (*e.g.*, a business associate agreement is in place if the vendor meets the definition of business associate).

In recent years, there has been significant public concern about the privacy practices of regulated entities, including the use of tracking technologies on their websites, which has been reflected in a spate of media reporting on regulated entities' data practices, lawsuits brought by private litigants arising from disclosures made through tracking technologies, academic papers, and regulatory efforts. *See, e.g.* AR227–41; AR260–62; AR301–04; AR347–49; AR426–46. This growing attention revealed significant differences in how regulated entities implemented the requirements of the HIPAA Rules in the context of online tracking technologies. *Compare, e.g.*, AR347–49 (covered entity denied that any PHI was disclosed through tracking), *with* AR248–59 (discussing covered entity's self-reporting of inadvertent disclosure of PHI through the use of a tracking technology, including contact information, IP addresses, and "information such as

appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes").

Accordingly, OCR issued the original Bulletin to remind regulated entities of their obligations under the HIPAA Rules when they use online tracking technologies. On March 18, 2024, OCR replaced the original Bulletin with the Revised Bulletin to provide additional clarity about when visits to unauthenticated web pages may or may not disclose PHI to tracking technologies, additional tips for complying with the HIPAA Rules when utilizing tracking technologies, and additional information about OCR's enforcement priorities in the context of tracking technologies. AR1–17. Like the original Bulletin, the Revised Bulletin addresses the application of the HIPAA Rules in the specific contexts of "user-authenticated" and "unauthenticated" webpages. AR4–7.[4] Tracking technologies on user-authenticated webpages—webpages that require users to log in before accessing the page, such as patient portals—will "generally have access to PHI." AR4–5. For example, technologies used on those webpages can collect and disclose "diagnosis and treatment information, prescription information, billing information," patient status, and other information disclosed by the user, which can then be linked to an individual's "IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage." AR4.

By contrast, tracking technologies on "many unauthenticated webpages"—webpages that do not require users to log in—"do not have access to individuals' PHI." AR5. However, in some cases, tracking technologies on such pages "may have access to PHI." *Id.* The Revised Bulletin

[4] The Revised Bulletin also addresses the use of tracking technologies on mobile apps, *see* AR7–8, which Plaintiffs have not challenged here. *See* Pls.' Br. in Supp. of Mot. for Summ. J. ("Pls.' Br.") at 6 n.2, ECF No. 25.

advises that "regulated entities that are considering the use of online tracking technologies should consider whether any PHI will be transmitted . . . and take appropriate steps consistent with the HIPAA Rules." *Id.* To assist regulated entities in complying with their obligations, the Revised Bulletin provides several examples of "when visits to an unauthenticated webpage may or may not involve the disclosure of PHI." AR5–7. For example, visits to unauthenticated webpages that do not contain information that relates to an individual's health, health care, or payment for health care—like webpages that provide information about a "hospital's job postings or visiting hours"—would not involve the disclosure of PHI, even if information disclosed to tracking technologies could be used to identify an individual who visited that webpage. AR6. Visits to unauthenticated webpages that do not relate to an individual's past, present, or future health, health care, or payment for health care, also do not result in disclosure of PHI to a tracking technology. *Id.* Thus, if a student visited a hospital's webpage listing the oncology services the hospital provided for the purpose of researching a term paper, that would not constitute a disclosure of PHI even if the information could be used to identify the student. *Id.* Conversely, if an individual visited the same webpage listing oncology services for the purpose of seeking "a second opinion on treatment options for their brain tumor," transmission of that individual's identifying information could constitute a disclosure of PHI where the information was "both identifiable and related to the individual's health or future health care." *Id.* Along these same lines, tracking technologies on webpages that allow individuals to schedule appointments with providers or use a symptom-checker tool may have access to PHI where the individual's identifying information—such as their email address or IP address—is transmitted in connection with this information related to their health or future health care. AR7. In addition, webpages that request, but do not require, login

information are not themselves user-authenticated, but a tracking technology that collects the user's login credentials may have access to PHI. *Id.*

Having alerted regulated entities to situations in which they need to consider the risks of PHI being disclosed, the Revised Bulletin then reminds regulated entities of their obligation to "comply with the HIPAA Rules when using tracking technologies." AR8. It counsels regulated entities that the Privacy Rule requires either "[e]nsuring that all disclosures of PHI to tracking technology vendors are specifically permitted" or obtaining authorization for disclosures of PHI. AR9–10. It also reminds regulated entities that the Privacy Rule contains several methods of compliance allowing regulated entities to disclose PHI to third parties through tracking technologies. *Id.* The Privacy Rule permits, for example, disclosures of PHI to business associates for specific purposes when a business associate agreement is in place, meaning that a regulated entity can disclose PHI to a business associate third-party tracking technology vendor so long as assurances to safeguard PHI are established. *Id.* The Revised Bulletin also informs regulated entities that, if a preferred tracking technology vendor will not enter into a business associate agreement, the regulated entity may comply with HIPAA by entering into such an agreement with a vendor that will de-identify information before providing information to that tracking technology vendor. *Id.* In addition, in the absence of a business associate relationship, the Privacy Rule still permits regulated entities to disclose PHI to vendors with individuals' authorizations in accordance with 45 C.F.R. § 164.508. *Id.*

The Revised Bulletin also informs regulated entities about OCR's enforcement priorities. It shares that OCR is "prioritizing compliance with the HIPAA Security Rule," which "helps lower the risk of unauthorized access" to PHI "that could lead to harm to individuals." AR11. The Revised Bulletin points out that OCR investigations are "fact-specific" and that the agency

"considers all of the available evidence in determining compliance and potential remedies for noncompliance." *Id.* Finally, the Revised Bulletin states specifically that it "do[es] not have the force and effect of law" and is "not meant to bind the public in any way." *Id.*

PROCEDURAL HISTORY

On November 2, 2023, Plaintiffs—two trade associations representing hospitals, health care systems, networks, and other health care providers, along with two health systems—filed this action challenging only the portion of the Revised Bulletin that relates to the use of online tracking technologies on unauthenticated pages that do not request login credentials. *See* Compl. ¶¶ 27–30, 40, ECF No. 1. Pursuant to the parties' joint motion, the Court waived Defendants' requirement to respond to the Complaint. *See* Order, ECF No. 22.

On January 5, 2024, Plaintiffs moved for summary judgment on three grounds. They first argue that the challenged provisions of the Revised Bulletin exceed HHS's statutory authority because they are allegedly inconsistent with HIPAA's definition of IIHI. *See* Pls.' Br. at 16–23. Second, Plaintiffs argue that the Revised Bulletin is arbitrary and capricious. *Id.* at 27–30. Third, Plaintiffs argue that the Revised Bulletin is a substantive rule that was issued without notice-and-comment procedures. *Id.* at 30–34.

LEGAL STANDARD

The Court's review of Plaintiffs' challenge to the Revised Bulletin is restricted to the administrative record before the agency. *See* Order, ECF No. 22. When the record establishes "that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law," summary judgment is appropriate. Fed. R. Civ. P. 56(a); *see also Amin v. Mayorkas*, 24 F.4th 383, 391 (5th Cir. 2022) (noting that APA claims are generally resolved at summary judgment).

ARGUMENT

I. THE COURT LACKS JURISDICTION OVER PLAINTIFFS' CLAIMS.

Plaintiffs' claims fail at the threshold for want of subject matter jurisdiction. Under the APA, the Court lacks jurisdiction to review the Revised Bulletin because it does not constitute final agency action.

A. The Revised Bulletin Is Not Final Agency Action.

The APA grants federal courts jurisdiction only over "final agency action." *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 882 (1990); *Qureshi v. Holder*, 663 F.3d 778, 781 (5th Cir. 2011) ("If there is no final agency action, a federal court lacks . . . jurisdiction." (citation omitted)); *see also* 5 U.S.C. § 704. Agency action is final if it (1) represents "the 'consummation' of the agency's decisionmaking process," and (2) conclusively determines legal "rights or obligations." *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (citations omitted). The Revised Bulletin satisfies neither requirement. It does not establish the agency's final position with respect to any concrete circumstances. It also lacks any independent force of law, as it explicitly states that it is non-binding and any legal consequences would only result after an administrative proceeding subject to judicial review. Accordingly, the Revised Bulletin does no more than "merely restate" a regulatory requirement or "merely reiterate what has already been established." *Nat'l Pork Producers Council v. U.S. EPA*, 635 F.3d 738, 756 (5th Cir. 2011); *see also Rhea Lana, Inc. v. Dep't of Labor*, 824 F.3d 1023, 1028 (D.C. Cir. 2016) (agency action was not final because it "created no new legal obligations beyond those [the statute] already imposed").

"Agency action may mark the consummation of the agency's decisionmaking process if the agency action 'is not subject to further agency review,'. . . which occurs when the agency has 'asserted its final position on the factual circumstances underpinning' the agency action."

Louisiana v. U.S. Army Corps of Eng'rs, 834 F.3d 574, 581 (5th Cir. 2016) (citations omitted). The Revised Bulletin states that while tracking technologies on "many" unauthenticated webpages "do not have access to individuals' PHI," tracking technologies on unauthenticated webpages that address health conditions or allow individuals to search for doctors or appointments "may have access to PHI in certain circumstances." AR5–7. It does not, however, assert a "final position" on any "factual circumstances." *Louisiana*, 834 F.3d at 581. Rather, the agency's final position regarding the fact-specific question of whether any regulated entity's particular conduct violated the HIPAA Rules would come only after an investigation by OCR and a separate administrative enforcement proceeding. *See supra* pp. 8–9; *see also Peoples Nat'l Bank v. Off. of Comptroller of Currency of the U.S.*, 362 F.3d 333, 337 (5th Cir. 2004) ("[A] non-final agency order is one that 'does not of itself adversely affect [plaintiffs] but only affects [their] rights adversely on the contingency of future administrative action.'" (citation omitted)).

Plaintiffs make much of the original Bulletin's inclusion of a single illustrative example of conduct—the collection of an email address or IP address of an individual who visits a webpage for the purpose of "search[ing] for available appointments with a health care provider"—to outline one hypothetical situation in which a tracking technology vendor would likely have access to PHI in the context of an unauthenticated webpage. But in the Revised Bulletin, OCR has now provided additional examples clarifying when a regulated entity might disclose PHI to a tracking technology. AR6–7. And in any event, the example Plaintiffs latch onto is divorced from the factual context of any particular case, including the contents of the hypothetical webpage involved or the information that is actually collected by the hypothetical tracking technology. *See* AR3 (explaining that types of online tracking technologies vary); *see also* AR231–33 (discussing various tracking technologies and the different types of information collected by each). It is not

sufficiently concrete to constitute the consummation of the agency's decisionmaking. *Exxon Chems. Am. v. Chao*, 298 F.3d 464, 467 (5th Cir. 2002) (agency action was not final where agency "has not issued a decision definitively resolving the merits of [the] case"); *see also Spring Branch Wildlife Preserve v. U.S. EPA*, No. 3:20-cv-225, 2021 WL 6503917, at *3 (S.D. Tex. Sept. 17, 2021) (agency letter was not final agency action where it "outline[d] a range of possible enforcement options, but stops short of committing itself to any particular action," and agency was free to mandate restoration of wetlands, seek civil penalties, do both, or "take no action at all"), *aff'd*, No. 22-40031, 2022 WL 9914735 (5th Cir. Oct. 17, 2022) (per curiam).

The Revised Bulletin is also not final because it does not create any new legal rights or obligations. Instead, it merely reiterates the Privacy Rule's longstanding restrictions on the use and disclosure of PHI to third parties, and highlights certain other preexisting obligations under the Security and Breach Notification Rules. As the Revised Bulletin explains, "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors." AR2; *see also* 45 C.F.R. § 164.502(a) (restricting covered entities from disclosing PHI to third parties except as specifically authorized). HHS has always interpreted the Privacy Rule as providing that there is a reasonable basis to believe that certain categories of information—including email addresses and IP addresses—can be used to identify individuals, *see* 45 C.F.R. § 164.514(b), and such identifying information is PHI when tied to information that reflects an individual's health or health care, *see id.* § 160.103. Indeed, the examples included in the Revised Bulletin—such as the collection of an email address from an individual who visits a webpage and "makes an appointment with a health care provider" or "enters symptoms in an online tool to obtain a health analysis"—is precisely the sort of information that the HIPAA Rules have always protected. *See* AR7. Thus, rather than breaking new ground, the Revised Bulletin simply

"highlight[s] the obligations" of regulated entities that already exist under the HIPAA Rules, clarifies that those obligations apply to disclosures to tracking technologies, and reminds regulated entities that the Privacy Rule permits them to disclose PHI to tracking technology vendors by entering into business associate agreements or obtaining individuals' authorizations. AR1–10. Plaintiffs suggest that prior to the original Bulletin, the use of online tracking technology "was not affected by HIPAA," Pls.' Br. at 2, but that is simply incorrect. Disclosures made to third parties through online tracking technologies have never been exempt from the basic requirements of the HIPAA Rules, even if some covered entities may have wrongly assumed otherwise. Indeed, other entities self-reported disclosures of PHI to tracking technologies before the original Bulletin was issued. *See* AR248–59; AR276–78; AR283–85.

Furthermore, no legal consequences flow from the Revised Bulletin itself. The Revised Bulletin explicitly states that it "do[es] not have the force and effect of law" and is "not meant to bind the public in any way." AR11. While such disclaimers are not dispositive of finality, the Revised Bulletin's explanation of its legal effect is bolstered by the fact that any legal consequences require an administrative enforcement proceeding, which would then be subject to judicial review. *See AT&T Co. v. EEOC*, 270 F.3d 973, 976 (D.C. Cir. 2001) (agency's expressed "view of the law" is non-final when it "has force only to the extent the agency can persuade a court to the same conclusion") The Revised Bulletin clarifies how OCR understands the HIPAA Rules to apply to the use of tracking technologies, but it does not itself impose any legal duties, all of which flow directly from the HIPAA Rules. *See Luminant Generation Co. v. U.S. EPA*, 757 F.3d 439, 442 & n.7 (5th Cir. 2014) (agency action is not final if "an agency merely expresses its view of what the law requires of a party, even if that view is adverse to the party" (citation omitted)).

Nor does the Revised Bulletin bind HHS to any particular legal position. "Courts . . . determine whether agency action binds the agency by looking for (1) mandatory language, (2) actions that restrict the agency's discretion to adopt a different view of the law, and (3) the creation of safe harbors from legal consequences." *Texas v. Becerra*, 89 F.4th 529, 538 (5th Cir. 2024) (citation omitted). Contrary to Plaintiffs' suggestion, *see* Pls.' Br. at 25, the inclusion in the original Bulletin of a single hypothetical describing circumstances in which PHI could potentially be collected, *see* AR22, outside of the context of any particular case, does not create a mandate and does not fix OCR's legal position. *See Prof'ls & Patients for Customized Care v. Shalala,* 56 F.3d 592, 596–97 (5th Cir. 1995) ("As long as the agency remains free to consider the individual facts in the various cases that arise, then the agency action in question has not established a binding norm." (citing *Ryder Truck lines, Inc. v. United States*, 716 F.2d 1369, 1377 (11th Cir. 1983)). Moreover, the Revised Bulletin provides more examples, along with enforcement priorities, that make plain the case-specific nature of OCR investigations. AR5–7, 11. And the Revised Bulletin does not create any safe harbors; it merely directs covered entities to utilize methods of compliance that already exist under the HIPAA Rules. *See* AR9–10.

The Revised Bulletin is therefore distinguishable from the guidance documents at issue in the authorities upon which Plaintiffs rely. In *Becerra*, the Fifth Circuit held that an HHS guidance document addressing hospitals' obligations under Emergency Medical Treatment and Active Labor Act (EMTALA) was final agency action. 89 F.4th at 539–41. But central to the court's analysis was the fact that the guidance document was issued after the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022), which "caused a sea change in the law." *Becerra*, 89 F.4th at 541. Because of the "new ingredient" of *Dobbs*, the court concluded that the guidance did not "merely restate" EMTALA's preexisting requirements but set

out "for the first time" the agency's "legal position . . . regarding how EMTALA operates post-*Dobbs*." *Id.* Here, in contrast, there has been no change in the law. The Revised Bulletin merely clarifies that the longstanding obligations of the HIPAA Rules apply in the context of online tracking technologies.

The Fifth Circuit's decision in *Texas v. EEOC*, 933 F.3d 433 (5th Cir. 2019), is similarly distinguishable. There, the court held that an EEOC guidance document constituted final agency action where the guidance bound EEOC staff to a particular "analytical method in conducting Title VII investigations," "limit[ed] discretion respecting the use of certain evidence," "direct[ed] their decisions about which employers to refer for [employment] actions," and "le[ft] no room for EEOC staff *not to*" take certain actions. *Id.* at 443. By contrast, the Revised Bulletin does not require OCR to adopt any method for conducting investigations—or indeed to take any action at all. The single illustrative hypothetical, upon which Plaintiffs' finality argument rests, *see* Pls.' Br. at 25—and which has now been replaced with additional, more nuanced hypotheticals—bears little resemblance to the detailed and comprehensive document at issue in *EEOC*.

The non-binding district court cases Plaintiffs cite are also inapposite. *See* Pls.' Br. at 24–26 (citing *Texas v. Brooks-LaSure*, No. 6:23-cv-161, 2023 WL 4304749, at *8 (E.D. Tex. June 30, 2023) (guidance document was not reminder of agency's previously articulated position where agency had "on several occasions[] explicitly disclaimed" position adopted in guidance); *Texas v. HHS*, No. 23-cv-22, --- F. Supp. 3d ----, 2023 WL 4629168, at *10 (W.D. Tex. July 12, 2023) (guidance document issued after change in law resulting from *Dobbs* decision constituted final action); *Nat'l Fed'n of Indep. Bus. v. Dougherty*, No. 3:16-CV-2568, 2017 WL 1194666, at *7 (N.D. Tex. Feb. 3, 2017) (agency interpretive letter was final where it changed legal interpretation of statute and had been implemented against organizational plaintiff's members). None of these

decisions suggest that a mere reminder that preexisting legal obligations continue to apply in a particular context constitutes final agency action.

Finally, Plaintiffs cannot establish that the Revised Bulletin is final through references to compliance letters and public statements. *See* Pls.' Br. at 25. None of the cited materials instruct that parties must comply with the *Revised Bulletin*, as opposed to the underlying requirements of the *HIPAA Rules* themselves. *See* Pls.' App'x in Supp. of Mot. for Summ. J. ("Pls.' App'x") at 16–17, ECF No. 26 (stating that the original Bulletin "provides a general overview of how the HIPAA Rules apply . . . and reminds regulated entities of their obligations to comply with the *HIPAA Rules* when using tracking technologies," and advising recipient to "review *the laws* cited in this letter and take actions" accordingly (emphases added)); *id.* at 19–20 (noting that the original Bulletin "reminded entities covered by HIPAA of their responsibilities . . . under the law" and that investigations are ongoing "to ensure compliance *with HIPAA*").[5]

Thus, the Revised Bulletin does not constitute final agency action, and Plaintiffs cannot proceed under the APA.

B. Plaintiffs Cannot Avoid the Finality Requirement by Recasting a Garden-Variety APA Claim as a Non-statutory Equitable Claim.

In an apparent attempt to circumvent the finality requirement, Plaintiffs contend that their statutory-authority claim may proceed not only under the APA, but also as a non-statutory equitable claim (or, failing that, under the Declaratory Judgment Act). *See* Pls.' Br. at 15. This gambit should be rejected. Their central contention—that the challenged portion of the Revised Bulletin exceeds the agency's statutory authority—is a garden-variety APA claim. *See* 5 U.S.C.

[5] Plaintiffs also cite statements purportedly from a media interview with an acting OCR Deputy Director. *See* Pls.' Br. at 8. Although the link to the interview provided by Plaintiffs does not contain a working link to the video recording, the cited quotations, to the extent they are accurate, appear consistent with the cited portions of the other materials.

§ 706(2)(C) (authorizing a court to hold unlawful agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right"). Under these circumstances, it would be inappropriate to rely on an implied equitable cause of action, least of all on Plaintiffs' theory that the challenged action falls so far outside the scope of the agency's statutory authority as to render it *ultra vires*, a contention that "is essentially a Hail Mary pass—and in court as in football, the attempt rarely succeeds." *Nyunt v. Chairman, Broadcasting Bd. of Governors*, 589 F.3d 445, 449 (D.C. Cir. 2009) (Kavanaugh, J.).

1. Prior to the enactment of the APA, courts recognized the implied equitable authority to enjoin the actions of federal officials that exceed their statutory authority. *See Armstrong*, 575 U.S. at 327; *Fed. Exp. Corp. v. U.S. Dep't of Comm.*, 39 F.4th 756, 763–64 (D.C. Cir. 2022) (discussing development of non-statutory review of *ultra vires* actions); *see also Apter v. HHS*, 80 F.4th 579, 587–88 (5th Cir. 2023). Even if some form of *ultra vires* review survived the 1976 amendments to the APA—a question about which the Fifth Circuit has expressed significant doubt, *see Geyen v. Marsh*, 775 F.2d 1303, 1307 (5th Cir. 1985) (raising substantial doubt that *ultra vires* actions survive the 1976 amendments to the APA); *see also Apter*, 80 F.4th at 593 ("[U]nder our precedent, Congress apparently did away with the *ultra vires* doctrine and other fictions surrounding sovereign immunity when it amended the APA in 1976" (cleaned up))—Plaintiffs cannot satisfy the demanding standard required to bring an *ultra vires* claim.

"To invoke [an *ultra vires* action], a plaintiff must 'do more than simply allege that the actions of the officer are illegal or unauthorized.'" *Danos v. Jones*, 652 F.3d 577, 583 (5th Cir. 2011) (quoting *Ala. Rural Fire Ins. Co. v. Naylor*, 530 F.2d 1221, 1226 (5th Cir. 1976)). "[*U*]*ltra vires* claims are confined to extreme agency error where the agency has stepped so plainly beyond the bounds of its statutory authority, or acted so clearly in defiance of it, as to warrant the

immediate intervention of an equity court." *Fed. Exp.*, 39 F.4th at 764 (cleaned up). The challenged action must "go beyond mere legal or factual error and amount to a 'clear departure by the [agency] from its statutory mandate' or be 'blatantly lawless' agency action." *Id.* (quoting *Oestereich v. Selective Serv. Sys. Loc. Bd. No. 11*, 393 U.S. 233, 238 (1968)); *see also Danos*, 652 F.3d at 583 (plaintiff must "allege facts sufficient to establish that the officer was acting 'without any authority what[so]ever,' or without any 'colorable basis for the exercise of authority'" (quoting *Pennhurst State Sch. & Hosp. v. Halderman*, 465 U.S. 89, 101 n.11 (1984)); *Am. Airlines Inc. v. Hermann*, 176 F.3d 283, 293 (5th Cir. 1999) (*ultra vires* review is a "narrow exception" reserved for only the most "egregious error[s]"). "Only error that is 'patently a misconstruction of the Act,' that 'disregard[s] a specific and unambiguous statutory directive,' or that 'violate[s] some specific command of a statute' will support relief." *Fed. Exp.*, 39 F.4th at 764 (quoting *Griffith v. Fed. Labor Rel. Auth.*, 842 F.2d 487, 493 (D.C. Cir. 1988)).

Plaintiffs fall far short of clearing that high bar. They do not suggest that HHS lacks authority to issue guidance expressing its views about the requirements of the HIPAA Rules. *Cf. Apter*, 80 F.4th at 588 (concluding that plaintiffs established the "strong merits argument" court assumed was "needed to overcome sovereign immunity" because the Food and Drug Administration (FDA) lacked statutory power to offer medical advice). Rather, Plaintiffs rest their *ultra vires* claim on the argument that HHS is supposedly incorrectly interpreting the term IIHI in the context of tracking technologies on certain unauthenticated webpages. *See* Pls.' Br. at 15; *id.* at 16–20; *see also id.* at 1 (arguing the original Bulletin is "contrary to law because it restricts the use of information that is not protected under [HIPAA]"). Plaintiffs are wrong about that, *see infra* pp. 27–35, but regardless, what they are asserting is a garden-variety argument that an agency misinterpreted the operative statutory language. That cannot give rise to an *ultra vires* claim. *See*

Fed. Exp., 39 F.4th at 765 (plaintiff "must show more than the type of routine error" in statutory interpretation that would apply under the APA (citation omitted)); *Danos*, 652 F.3d at 583 (plaintiff must allege more than "that the actions of the officer are illegal or unauthorized" (citation omitted)).

Plaintiffs' effort to cast a plain-vanilla APA claim in the guise of an implied equitable *ultra vires* claim fails for the additional reason that such claims are available only where "there is no alternative procedure for review." *Nyunt*, 589 F.3d at 449 (citation omitted); *see also Leedom v. Kyne*, 358 U.S. 184, 190 (1958) (allowing implied equitable *ultra vires* claim where the "absence of jurisdiction . . . would mean a sacrifice or obliteration of a right which Congress has given [plaintiffs], for there is no other means . . . to protect and enforce that right" (citation omitted)). Here, Plaintiffs have an obvious alternative procedure for review: the APA. *See* 5 U.S.C. § 706(2)(C); *see also* Compl. ¶ 37. Courts confronted with parallel claims asserting the same statutory violations under both equitable and express statutory causes of action have dismissed the equitable claims. *See Am. Airlines*, 176 F.3d at 294 (dismissing *ultra vires* claim challenging non-final agency action because "[i]f and when the [agency] finds that [the plaintiff] has violated the Act and its regulations, [the plaintiff] will have . . . 'an unquestioned right to review of both the regulation and its application'" (quoting *Bd. of Governors. of Fed. Rsrv. Sys v. MCorp Fin., Inc.*, 502 U.S. 32, 43-44 (1991))); *Exxon Chems.*, 298 F.3d at 469 (similar); *see also Puerto Rico v. United States*, 490 F.3d 50, 59–60 (1st Cir. 2007) (dismissing non-statutory claim where APA provided plaintiff with the "means of vindicating its rights without nonstatutory review"); *Neb. State Legis. Bd. United Transp. Union v. Slater*, 245 F.3d 656, 659 (8th Cir. 2001) (plaintiff could not rely on *ultra vires* exception where it "had a meaningful and adequate opportunity for judicial review" through statutory review scheme, even when that claim was barred (citation omitted));

Jafarzadeh v. Duke, 270 F. Supp. 3d 296, 311 (D.D.C. 2017) ("[B]ecause plaintiffs are able to assert the same claim through the APA, they cannot obtain relief . . . through the Court's inherent power to review *ultra vires* agency actions.").

Allowing Plaintiffs to utilize the *ultra vires* exception to assert a mine-run challenge to agency action in order to circumvent the finality requirement would distort the judicial review scheme. There would be little reason for any plaintiff to rely on the APA or a specific statutory judicial review provision if it were free to bring an implied equitable action based on the same theory without having to comply with the limitations Congress imposed on those review provisions. *See* 33 Charles A. Wright & Arthur R. Miller, Fed. Prac. & Proc. § 8307 (3d ed. Apr. 2020 update) (recognizing that if implied causes of action were always available to challenge agency action, it would "raise[] the question of why anyone would bother to use more limited causes of action created by special statutory review proceedings and the APA"). That conclusion is consistent with the "doctrine of equity jurisprudence that courts of equity should not act . . . when the moving party has an adequate remedy at law." *Younger v. Harris*, 401 U.S. 37, 43 (1971); *see also FCC v. ITT World Commc'ns, Inc.*, 466 U.S. 463, 468 (1984) ("[l]itigants may not evade" a provision that vests the courts of appeals with exclusive jurisdiction by requesting a district court enjoin agency "action as ultra vires"); *Block v. N. Dakota ex rel. Bd. of Univ. & Sch. Lands*, 461 U.S. 273, 284–85 (1983) (plaintiffs could not avoid a statute of limitations or other restrictions by resorting to *ultra vires* claim).

Plaintiffs' reliance on the Fifth Circuit's decision in *Apter*, *see* Pls.' Br. at 15—which permitted the plaintiffs to move forward on a non-statutory cause of action, 80 F.4th at 590—is misplaced. To start, the plaintiffs in *Apter* alleged that the FDA lacked the statutory power to engage in the type of action in question. *See id.* at 588. By contrast, Plaintiffs here assert only a

routine argument that the agency misinterpreted the statute. Moreover, in *Apter*, the Government did not argue either in its motion to dismiss or on appeal that the plaintiffs had an adequate alternative procedure for review. *See* Mot. to Dismiss, *Apter v. HHS*, No. 3:22-cv-184, ECF No. 25; Br. for Appellees, *Apter v. HHS*, No. 22-40802, ECF No. 37; *see also Webster v. Fall*, 266 U.S. 507, 511 (1925) ("Questions which merely lurk in the record, neither brought to the attention of the court nor ruled upon, are not to be considered as having been so decided as to constitute precedents.").

Thus, Plaintiffs cannot invoke a non-statutory *ultra vires* claim to circumvent the finality requirement under the APA.

2. Nor can Plaintiffs rely on the Declaratory Judgment Act to provide them a cause of action where one would not . The Declaratory Judgment Act does not itself create an independent cause of action. *See, e.g.*, *Braidwood Mgmt., Inc. v. EEOC*, 70 F.4th 914, 933 (5th Cir. 2023); *Harris Cnty. v. MERSCORP Inc.*, 791 F.3d 545, 552 (5th Cir. 2015). "[T]he Act 'enlarged the range of remedies available in the federal courts,' but it did not create a new right to seek those remedies." *Harris Cnty.*, 791 F.3d at 552 (quoting *Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950)). Here, Plaintiffs do not assert that HHS would be "within its power to bring an enforcement action" in federal court against them. *See Braidwood*, 70 F.4th at 932; *see also id.* at 933 (explaining that "it is the underlying cause of action of the defendant against the plaintiff that is actually litigated in a declaratory judgment action"). They thus fail to show that "the independent cause of action required for a declaratory judgment exists." *Id.* at 932.

Accordingly, Plaintiffs cannot evade the APA's finality requirement by resort to the Declaratory Judgment Act.

II. PLAINTIFFS' CLAIMS FAIL ON THE MERITS.

Even if the Court had jurisdiction over Plaintiffs' claims, it should reject them on the merits. The Revised Bulletin's reminder that the HIPAA Rules apply to online tracking technologies is entirely consistent with the statutory definition of IIHI. Moreover, it is not arbitrary and capricious and did not require notice-and-comment procedures.

A. The Revised Bulletin Is Consistent with HIPAA's Definition of IIHI.

The Revised Bulletin's reminder that the HIPAA Rules apply to PHI collected by online tracking technologies on unauthenticated webpages is consistent with the statutory definition of IIHI. HIPAA and the HIPAA Rules both define IIHI to include: "any information" that (1) is created or received by a covered entity; (2) relates to the past, present, or future health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for health care; and (3) either identifies the individual or "with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103. In defining IIHI, Congress consciously used the expansive terms "relate[] to" and "reasonable basis to believe" to ensure that covered entities would broadly protect information about past, present, or future health conditions; health care; or payment for health care that might be able to identify the individuals linked to those health care needs. *See, e.g.*, Merriam-Webster's Dictionary (defining "relate" as having a "connection" and "relate to" as "to be connected with" or "to be about" something);[6] Black's Law Dictionary (11th ed. 2019) (defining "related" as "[c]onnected in some way"); *see also Beiser v. Weyler*, 284 F.3d 665, 669 (5th Cir. 2002) ("The phrase 'relates to' generally conveys a sense of breadth.").

[6] *See* https://www.merriam-webster.com/dictionary/relate; https://www.merriam-webster.com/dictionary/relate%20to.

The capacious definition of IIHI plainly can cover information collected by tracking technologies embedded on regulated entities' websites.[7] While not always the case, tracking technologies on unauthenticated webpages that either address specific health symptoms or conditions or allow searching for particular medical providers or appointments could have access to PHI when the information disclosed "is both identifiable and related to the individual's health or future health care." AR5–7. This guidance aligns with the text of HIPAA and the Privacy Rule. Indeed, tracking technologies capture information from users as they navigate to and interact with regulated entities' websites, meaning the users' information is "received by" a regulated entity. Those technologies can capture information that can be used to identify individuals, such as IP addresses, email addresses, and geographic locations. *See* 45 C.F.R. § 164.514 (listing these categories of information as individual "identifiers"). Indeed, the very point of tracking technologies is to *track* users. *See* AR227–28. And if an individual navigates to a website to log into a patient portal, to access information about their medical condition or symptoms, to look for a particular provider, or to seek a health care appointment, some of the information gathered by tracking technologies—such as the contents of the page, what buttons or links the user clicked, or any search terms the user may have employed—could disclose information about that individual's past, present, or future health care. *See In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 791–93 (N.D. Cal. 2022) (finding that a covered entity disclosed individuals' PHI to an online tracking technology on a patient portal login page).

[7] Plaintiffs expressly disclaim any challenge to the portions of the Revised Bulletin addressing online tracking technologies used on user-authenticated webpages or unauthenticated webpages that request login information. *See* Pls.' Br. at 6 n.2. As the Revised Bulletin explains, tracking technologies used on such pages (including patient portals), can capture information about everything from a user's actual diagnoses and treatment options to communications with medical providers to billing information, *see* AR4–5; AR227–28—all while linking that information directly to the user.

Take, for example, a hypothetical Ms. Doe who navigates to a hospital's homepage. Tracking Ms. Doe's path to most of the unauthenticated webpages she could visit from there—such as pages providing the hospital's visiting hours, the hospital's address and driving directions, or an alphabetical directory of all medical departments or providers—most likely would not, without more, result in the disclosure of PHI to a third-party tracking technology. Consider, however, a scenario in which Ms. Doe is searching for a particular medical provider at the hospital. From the homepage, she clicks on a link to a page entitled "Find a Doctor," enters "oncologist" into the search bar, and then through a drop-down menu of conditions filters for particular oncologists that specialize in reviewing abnormal mammograms. An online tracking technology employed on those webpages that collects each of those interactions—which are linked to Ms. Doe's IP address and geographic location, and potentially even her Facebook or Google account—could have access to PHI, even though Ms. Doe never entered any login credentials. Data transmitted to the tracking technology vendor could include information that has a connection with Ms. Doe's past, present, or future health care needs, and there is a reasonable basis to believe that the information can be used to identify her. *See Cousin v. Sharp Healthcare*, No. 22-cv-2040, 2023 WL 8007350, at *3 (S.D. Cal. Nov. 17, 2023) (concluding that plaintiffs plausibly alleged that a tracking technology used on a hospital's unauthenticated webpage collected PHI where tracker "connect[s] internet activity to a specific individual using IP addresses and Facebook credentials" and where plaintiffs used website to search for "doctors who specialize in [particular medical] conditions" and for "information about their conditions (i.e., symptoms, treatments, procedures)," and one plaintiff "booked an appointment to obtain treatment for a medical condition" on webpage).

Plaintiffs argue that tracking technologies used on unauthenticated webpages "can never" provide a reasonable basis to identify "the individual" to whose health care needs the information "relates." *See* Pls.' Br. at 17. That is supposedly because an individual reasonably identified by an IP or email address may be visiting a webpage for "generic reasons that are unrelated" to anyone's health care needs (*e.g.*, for research or quality control, or by error) or for reasons related to the health care needs of someone other than the individual. *Id.* at 17–18; *see also id.* at 19–20.

Plaintiffs' focus on hypothetical alternative reasons for visiting an unauthenticated webpage is a red herring. In fact, the Revised Bulletin specifically acknowledges that some individuals visiting webpages that address specific medical conditions may be there for non-health care reasons, and that those types of visits would not result in the disclosure of PHI. *See* AR6. But it is beyond dispute that some individuals who visit these sorts of webpages *are* doing so in connection with their own health care needs. *See* Compl. ¶ 5 (alleging that tracking technologies are used, *inter alia*, to "help[] community members to more easily navigate to healthcare information so that they can better manage their healthcare," "allow visitors to virtually tour the facilities where particular procedures are performed," and provide "information about where healthcare services are available"); *see also* Corrected Br. of Amici Curiae State Hosp. Ass'ns at 8–9, ECF No. 37 (similar). Common sense dictates that at least some users who visit these webpages—like our hypothetical Ms. Doe—are doing so to learn information about their own medical conditions, to inquire about specific medical practices or providers for the purpose of obtaining health care, to actually obtain an appointment with a particular provider, or for other reasons related to their own health care.

Indeed, Plaintiffs themselves have informed OCR that they utilize analytics to track increases in community members searching for certain types of vaccinations—such as for the flu

or COVID-19—in order to allocate resources to address expected future need for vaccinations. AR36. Of course, in acknowledging that the data is useful in predicting the number of individuals who will seek vaccines, Plaintiffs are implicitly recognizing that individuals are seeking this information on the web for the purpose of their own future health care needs. What is more, Plaintiffs are recognizing that the value they derive from this data—at least in some circumstances—stems directly from the fact that individuals' web searches are reflective of their future health care needs. And the collection of that information by tracking technologies, when it can be used to identify those individuals, is PHI.

Although tracking technologies on unauthenticated websites may collect identifying information from users who are not visiting the webpage for their health care needs, identifying information about users who *are* visiting the webpage for their health care needs constitutes IIHI. Examples included in the Revised Bulletin make this distinction plain. AR6–7. Because the nature of tracking technologies may make it difficult for regulated entities to disaggregate IIHI from non-IIHI when disclosing information to third-party vendors, it may be prudent for regulated entities to prevent disclosures of non-IIHI if that is the only way to ensure that they are not disclosing PHI to third parties in violation of the Privacy Rule. But this potential practical consequence of deploying tracking technologies does *not* indicate that the Revised Bulletin redefines IIHI to cover all information collected from any individual visiting a webpage addressing specific symptoms, medical conditions, or allowing users to search for providers or appointments.

Plaintiffs next point to language in the original Bulletin that explained that "IIHI collected on a regulated entity's website . . . generally is PHI, even if the individual does not have an existing relationship with the regulated entity" because "the information connects the individual to the regulated entity" and is thus "indicative that the individual has received or will receive health care

services or benefits from the covered entity." AR20–21; *see also* Pls.' Br. at 18. Plaintiffs read this language—which the Revised Bulletin modifies and clarifies—to suggest that the original Bulletin reflected a view that every visit to an unauthenticated webpage addressing medical conditions or allowing searches for providers or appointments necessarily "relates to" the health care needs of the user, *see* Pls.' Br. at 18–19 (arguing this language expands the requirement that IIHI must "relate[] to" an individual's health care needs to cover information that "*might* relate to an individual's health"). Not so. The Revised Bulletin makes clear that "the mere fact that an online tracking technology connects [an] IP address . . . with a visit to a webpage addressing specific health conditions or listing health care providers is *not* a sufficient combination of information to constitute IIHI" if that visit "is not related to an individual's past, present, or future health, health care, or payment for health care." AR4 (emphasis added). The Revised Bulletin illustrates this distinction by explaining that the transmission of information identifying "a student . . . writing a term paper" as having accessed a webpage about specific services provided by a hospital would not constitute PHI, whereas the transmission of information identifying an individual looking at the same webpage "to seek a second opinion on treatment options for their brain tumor" would. AR6.

Understood properly, the language to which Plaintiffs point—and particularly the portion that the Revised Bulletin retains—merely states that an "existing relationship" between an individual and a regulated entity is not a prerequisite for information to constitute PHI. It is not unusual for the HIPAA Rules to protect IIHI acquired by a covered entity regardless of whether an existing relationship between the entity and the individual exists. For example, if a primary care physician were to refer a patient to a particular cardiologist, and the patient provided certain basic health and insurance information to the cardiologist before deciding on a different course of

treatment, the Privacy Rule would require the cardiologist to maintain the privacy of that information, even though the cardiologist has no existing relationship with the patient. That is because, despite the absence of any existing relationship, the information connects the patient with the cardiologist—and indicates that the patient needs cardiology care—and thus relates to the patient's past, present, or future health or health care. Similarly, IIHI collected on a covered entity's website, whether from a patient portal or certain unauthenticated webpages, may constitute PHI even if there is not an "existing relationship" between the user and the covered entity. AR4.

Plaintiffs' other arguments fare no better. Plaintiffs argue that the Revised Bulletin "disregard[s] the HIPAA balance" between promoting efficiency in health care and protecting privacy by failing to give due consideration to the beneficial uses of tracking technologies. Pls.' Br. at 20. But while there could be benefits from the freer disclosure of PHI, as the Privacy Rule itself recognizes, regulated entities are incentivized to "over-use" PHI because they reap the full benefits from the disclosures but do not "bear a significant share . . . of the cost to patients (in terms of lost privacy)." 65 Fed. Reg. at 82762. That is why the Privacy Rule strikes a careful balance by generally restricting the disclosure of PHI except for specific and limited purposes that promote the efficient provision of high-quality health care. *See, e.g.*, 45 C.F.R. § 164.502(a). The Revised Bulletin specifically acknowledges the potential benefits of using tracking technologies, and reminds regulated entities that, while they enjoy these benefits, they remain responsible for protecting PHI in situations where it may be collected through tracking technologies. AR3–11. Far from being novel, this reminder merely reiterates the same balance between privacy and efficiency that has always been reflected in the Privacy Rule.

Furthermore, neither the HIPAA Rules nor the Revised Bulletin prevent Plaintiffs from using tracking technologies. There is nothing in the HIPAA Rules or the Revised Bulletin that

bars Plaintiffs, their members, or any other regulated entities from using tracking technologies to "help improve care or the patient experience," Pls.' Br. at 20 (quoting AR20), consistent with their obligation to protect PHI. To the contrary, the Revised Bulletin provides regulated entities guidance about how they might deploy tracking technologies in a manner that complies with the HIPAA Rules. AR8–11. For example, regulated entities can permissibly disclose PHI to third parties through tracking technologies by entering into business associate agreements with third-party tracking technology vendors or with vendors who can de-identify data before transferring it to tracking technology vendors. *See id.*; *see also* 45 C.F.R. § 164.502(a)(4) (permitting disclosures to business associates); *id.* § 164.514 (permitting disclosure of de-identified data). Or they could seek valid authorizations from users. *See id.* § 164.502(a)(1)(iv). But regulated entities may not disclose PHI to third-party vendors without complying with the HIPAA Rules.

Plaintiffs next argue that courts have "rejected . . . the interpretation underlying" the Revised Bulletin in cases brought by private litigants against hospital systems and tracking technology companies for disclosures of information through tracking technologies. *See* Pls.' Br. at 21. These cases are all non-binding and engage only in a cursory analysis of the statutory language, without the benefit of the Government's participation. *See Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018); *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 4707184, at *3–4 (N.D. Ill. July 24, 2023); *Hartley v. Univ. of Chi. Med. Ctr.*, No. 22 C 5891, 2023 WL 7386060, at *2 (N.D. Ill. Nov. 8, 2023). The Court should decline to follow them. *See Cousin*, 2023 WL 8007350, at *3 (concluding that web tracker on unauthenticated page captured PHI).

Nor can Plaintiffs establish inconsistency between the Revised Bulletin and the statutory text by pointing to extra-record evidence to suggest that certain federal agency websites use tracking technologies. *See* Pls.' Br. at 21. To the extent any federal agencies are using tracking

technologies that collect information relating to a user's past, present, or future health care needs and which can be used to identify the user, the Revised Bulletin reminds them to protect that information consistent with the requirements of the HIPAA Rules, just as it does for regulated entities outside of the federal government.

Finally, Plaintiffs invoke the canon of constitutional avoidance to suggest that any interpretation of IIHI that covers information collected on unauthenticated websites raises "serious constitutional concerns that the Revised Bulletin abridges health care providers' own First Amendment rights." *Id.* But the constitutional avoidance canon "has no application in the absence of statutory ambiguity," *United States v. Oakland Cannabis Buyers' Co-op.*, 532 U.S. 483, 494 (2001), and as discussed above, tracking technologies on certain types of unauthenticated pages can collect information that relates to users' past, present, or future health care needs and that can be used to identify those users, *see supra* pp. 27–31. There is no statutory ambiguity, as that information fits neatly within the statutory definition of IIHI.

Even if there were ambiguity, the interpretation set out in the Revised Bulletin presents no serious constitutional concerns. Plaintiffs rely on the Supreme Court's decision in *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), to argue that the Revised Bulletin amounts to a content-based restriction on speech to which strict scrutiny must apply. Pls.' Br. at 22–23. But that is the wrong standard. Even assuming *arguendo* that a restriction on disclosure of information captured by tracking technologies is a regulation of speech rather than conduct and that any such restriction is content-based, it does not follow that strict scrutiny would apply. *See Sorrell*, 564 U.S. at 571–72 (declining to apply strict scrutiny to restriction on speech that was both "content based and . . . viewpoint discriminatory").

To the extent the interpretation in the Revised Bulletin were understood to regulate speech, that speech—consisting of information compiled from current or potential customers that is disclosed to third parties pursuant to a contractual relationship, for the purpose of "provid[ing] better information" about health care services on offer, Pls.' Br. at 9—is commercial in nature. *See, e.g.*, *Boelter v. Hearst Commc'ns Inc*., 192 F. Supp. 3d 427, 445–46 (S.D.N.Y. 2016) (state law restricting disclosure of personally identifiable information regulated commercial speech because the information "relays an individual's economic decisions, elucidates an individual's economic preferences, and facilitates the proposal of new commercial transactions," and "businesses' increasing ability to profit from the collection and sale of data supports the conclusion that disclosing consumer information is—primarily, if not entirely—an economic act" (citation omitted)); *see also U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1233 n.4 (10th Cir. 1999) (internal business communications intended "to facilitate the marketing of telecommunications services" constituted commercial speech); AR227–28 (noting that tracking technologies are frequently employed to "track user behavior on the web for . . . advertising").

The constitutionality of restrictions on commercial speech is analyzed not under strict scrutiny but under the more permissive intermediate scrutiny standard set forth in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980). *See Hearst*, 192 F. Supp. 3d at 447 (applying *Central Hudson* standard to restriction on disclosure of personally identifiable information to data miners); *Boelter v. Advance Mag. Publ'rs Inc.*, 210 F. Supp. 3d 579, 598–99 (S.D.N.Y. 2016) (same). Where the speech concerns lawful activity and is not misleading, the *Central Hudson* standard looks to whether the restriction is justified by a substantial governmental interest, whether it directly advances that interest, and whether it is

"narrowly drawn" and not more extensive than necessary to serve the interest. *See, e.g.*, *Am. Acad. of Implant Dentistry v. Parker*, 860 F.3d 300, 307 (5th Cir. 2017).

The Revised Bulletin's interpretation of HIPAA readily passes muster under that standard. First, the government's interest in protecting the privacy of consumers' health information is plainly substantial. *See, e.g.*, 65 Fed. Reg. at 82465–68 (discussing harms from loss of privacy, which inhibit reaping "the full benefits of electronic technologies," and the need for privacy protections to ensure "the effective delivery of health care, both to individuals and to populations"); *see also Trans Union Corp. v. FTC*, 245 F.3d 809, 818 (D.C. Cir. 2001) (finding government's "interest [in] protecting the privacy of consumer credit information . . . is substantial"); *Hearst*, 192 F. Supp. 3d at 448 (state interest in preventing unauthorized disclosure of personally identifiable information was substantial). Second, the understanding set out in the Revised Bulletin directly advances that interest, as it reflects that HIPAA restricts disclosure by the entities that, other than the users themselves, are "those most likely to possess and collect that information," which "reduces the likelihood of consumers' private details becoming public." *Hearst*, 192 F. Supp. 3d at 449. Third, the Revised Bulletin's interpretation is narrowly drawn, consistent with HIPAA and the HIPAA Rules. *See Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989) (government must show a fit between interest and law's restrictions that is "not necessarily perfect," but rather "reasonable"). Tracking these longstanding regulations, it reflects that the statute is targeted at the entities most likely to possess sensitive information, and it contains several exceptions that authorize disclosures to third parties for specific purposes, *see* 45 C.F.R. § 164.502(a), including exceptions that would permit covered entities to disclose PHI to third-party tracking technology vendors through either business associate agreements or pursuant to individuals' authorizations, *see* AR8–10. Indeed, in *Sorrell* itself, the Court specifically

identified the Privacy Rule, which permits disclosure of sensitive information "in only a few narrow and well-justified circumstances," as an example of a permissibly tailored regulation. 564 U.S. at 573.

In sum, Plaintiffs have not identified any inconsistency between the Revised Bulletin and HIPAA's statutory text. Accordingly, the Court should reject Count One.

B. The Revised Bulletin Is Not Arbitrary and Capricious.

Plaintiffs also argue that they are entitled to summary judgment because the Revised Bulletin is the product of arbitrary and capricious decisionmaking. *See* Pls.' Br. at 27–30. However, the Revised Bulletin expresses a reasonable—and, indeed, correct—explanation of what HIPAA and the HIPAA Rules have long required.

The APA's arbitrary and capricious standard is "narrow and highly deferential." *Sierra Club v. U.S. Dep't of Interior*, 990 F.3d 909, 913 (5th Cir. 2021) (quoting *Medina Cnty. Env't Action Ass'n v. Surface Transp. Bd.*, 602 F.3d 687, 699 (5th Cir. 2010)). In applying the standard, a court "is not to substitute its judgment for that of the agency." *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). "A court simply ensures that the agency has acted within a zone of reasonableness and, in particular, has reasonably considered the relevant issues and reasonably explained the decision." *FCC v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021).

Plaintiffs principally argue that the Revised Bulletin is unreasonable because it offered "no explanation whatsoever" to support the conclusion that connecting a user's IP address to an unauthenticated webpage with specific health-related content can satisfy the statutory definition of IIHI. *See* Pls.' Br. at 28 (citation omitted). But on APA review, courts must uphold a "decision [of] less than ideal clarity . . . if the agency's path may reasonably be discerned." *Alaska Dep't of*

Env't Conservation v. EPA, 540 U.S. 461, 497 (2004) (citation omitted). That standard is more than met here. The Revised Bulletin provides a detailed discussion of tracking technologies and the sorts of information that they can gather, replete with citations to the relevant regulatory text. AR3–8. And it incorporates for comparative purposes examples of circumstances in which it is unlikely that a tracking technology would capture PHI, and those when a tracking technology could capture PHI. AR4–8. These examples are squarely consistent with the statutory language. *See supra* pp. 27–35. No further explanation was required. *See Prometheus*, 592 U.S. at 423 (agency decision need only be "reasonably explained").

Plaintiffs' argument that the Revised Bulletin reflects an unacknowledged change in position, *see* Pls.' Br. at 29, fails for the same reason. The Revised Bulletin does not change the definition of IIHI—it merely highlights and provides guidance about how the HIPAA Rules apply to online tracking technologies. The fact that some entities filed breach reports with OCR regarding the use of tracking technologies before the original Bulletin was published underscores this point. Nor can Plaintiffs manufacture a purported "inconsistency" in the application of the HIPAA Rules, *see id.*, simply by asserting that some federal agencies use tracking technologies.

Finally, Plaintiffs argue that the Revised Bulletin fails to establish that the costs of complying with HIPAA's requirements with respect to tracking technologies is justified by the privacy benefits. *See* Pls.' Br. at 29–30. But they cite no statutory provision requiring that sort of cost-benefit analysis for every agency action, much less in a mere guidance document. *See Michigan v. EPA*, 576 U.S. 743, 752 (2015) (although when "[r]ead naturally in . . . context" in the Clean Air Act, the statutory phrase "'appropriate and necessary' requires at least some attention to cost," there are "undoubtedly settings" in which it "does not"). Regardless, the relevant balance was struck long ago in HIPAA and the Privacy Rule. Indeed, the Privacy Rule has always

recognized that, notwithstanding the benefits of the electronic transmission of health information, the protection of PHI is essential for the provision of health care, and the loss of privacy imposes significant harms on health care consumers, exposing them to threats of "theft," "embarrassment," and unwanted intrusion into the sensitive details of their lives. 65 Fed. Reg. at 82,464–65; *see also* AR3 (listing "misinformation, identity theft, stalking, and harassment" as harms from disclosure of PHI through tracking technologies). Moreover, because entities "gain[] the full benefit[s] of using such information" but "do[] not suffer the losses from disclosure" of PHI, the incentives for regulated entities "discourage privacy protection." 65 Fed. Reg. at 82,761. Thus, the Privacy Rule strikes a "balance [between] the needs of the individual [and] the needs of the society," *id.* at 82,464, by allowing the disclosure of PHI only for certain specific uses—including through business associate agreements or pursuant to valid authorizations. In issuing the Revised Bulletin, OCR was entitled to rely on the harms identified by the Privacy Rule and the balance struck therein between the benefits of collecting and using PHI and the costs to consumers. *See Nat'l Ass'n of Mfrs. v. SEC*, 748 F.3d 359, 369–70 (D.C. Cir. 2014) (agency could rely on "Congress['s] conclu[sion], as a general matter," that rule's "costs were necessary and appropriate in furthering" statutory goals (citation omitted)); *see also Consumer Elecs. Ass'n v. FCC*, 347 F.3d 291, 303 (D.C. Cir. 2003) (rule that "court is not to substitute its judgment for that of the agency" is "especially true when the agency is called upon to weigh the costs and benefits of alternative policies" (citation omitted).

Accordingly, the Revised Bulletin is well within the zone of reasonableness, and the Court should reject Plaintiffs' claim that the Revised Bulletin is arbitrary and capricious.

C. The Revised Bulletin Did Not Require Notice-and-Comment Procedures.

Plaintiffs' final argument is that the challenged portion of the Revised Bulletin amounts to a legislative rule that could only be issued pursuant to notice-and-comment rulemaking procedures. *See* Pls.' Br. at 30–34. That is incorrect. The APA expressly exempts "interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice" from notice-and-comment rulemaking. 5 U.S.C. § 553(b)(A). As a policy statement, the Revised Bulletin is exempt from notice-and-comment procedures.

Policy statements are generally defined in contrast to "substantive" rules. Substantive rules have "the force and effect of law," *Perez v. Mortg. Bankers Ass'n*, 575 U.S. 92, 96 (2015) (quoting *Chrysler Corp. v. Brown*, 441 U.S. 281, 302–03 (1979)), while policy statements are "issued by an agency to advise the public prospectively of the manner in which the agency proposes to exercise a discretionary power," *Lincoln v. Vigil*, 508 U.S. 182, 197 (1993) (quoting *Chrysler Corp.*, 441 U.S. at 302 n.31). The Fifth Circuit "evaluate[s] two criteria to distinguish policy statements from substantive rules: whether the rule (1) imposes any rights or obligations and (2) genuinely leaves the agency and its decision-makers free to exercise discretion." *Flight Training Int'l, Inc. v. FAA*, 58 F.4th 234, 242 (5th Cir. 2023) (quoting *Texas v. United States*, 809 F.3d 134, 171 (5th Cir. 2015)).

Here, for many of the reasons discussed above, the Revised Bulletin is not a substantive rule. The Revised Bulletin does "not have the force and effect of law," as it explicitly states. *See* AR11. It does not impose any new legal rights or obligations, as any consequences from a regulated entity's use of online tracking technologies on an unauthenticated webpage flow from the HIPAA Rules themselves. Moreover, the Revised Bulletin does not remove discretion from agency decisionmakers with respect to any particular case or bind them to take any specific action.

Indeed, the Revised Bulletin includes guidance about OCR's enforcement priorities, further emphasizing that the agency plans to exercise its enforcement discretion to focus on compliance with the Security Rule, which helps to lower the risk of unauthorized access to PHI that "could lead to harm to individuals," that its investigations are "fact-specific," and that it "considers all available evidence in determining compliance and remedies for potential noncompliance," AR11—quintessential statements of policy.

Even if the Revised Bulletin were considered a substantive rule, it would at most be an interpretive rule and thus still exempt from notice-and-comment procedures. *See Flight Training Int'l*, 58 F.4th at 241 n.5 ("[T]he requirement of notice and comment attaches only to rules that are both 'substantive' and 'legislative.'"). Interpretive rules are "issued by an agency to advise the public of the agency's construction of the statutes and rules which it administers." *Perez*, 575 U.S. at 97 (quoting *Shalala v. Guernsey Mem'l Hosp.*, 514 U.S. 87, 99 (1995)). "In contrast to legislative rules, which 'effect[] a substantive change in existing law or policy,' interpretive rules 'clarify a statutory or regulatory term, remind parties of existing statutory or regulatory duties, or 'merely track[]' preexisting requirements and explain something the statute or regulation already required." *POET Biorefining, LLC v. EPA*, 970 F.3d 392, 407 (D.C. Cir. 2020) (quoting *Mendoza v. Perez*, 754 F.3d 1002, 1021 (D.C. Cir. 2014)); *see also Brown Exp., Inc. v. United States*, 607 F.2d 695, 700 (5th Cir. 1979) ("Generally speaking, . . . legislative rules are those which create law, . . . whereas interpretative rules are statements as to what the administrative officer thinks the statute or regulation means." (citation omitted)). To distinguish between the two types of substantive rules, the Fifth Circuit looks to (1) "whether the agency intended to speak with the force of law," (2) whether the rule is published in the Code of Federal Regulation, (3) "whether the agency 'explicitly invoked its general legislative authority,'" (4) "whether the agency claimed

Chevron deference," and (5) "whether the rule will produce significant effects on private interests." *Mock v. Garland*, 75 F.4th 563, 580 (5th Cir. 2023) (cleaned up).

Here, the weight of these factors demonstrate that the Revised Bulletin is not a legislative rule. As discussed, the Revised Bulletin does not speak with the force of law, and it explicitly disclaims having a binding effect. *See supra* pp. 18–19. It does not create any new law, but rather reminds regulated entities that their preexisting duties under the HIPAA Rules apply to online tracking technologies, including on unauthenticated webpages. The Revised Bulletin was not published in the Code of Federal Regulations (notwithstanding Plaintiffs' curious suggestion that this factor could be met by press releases and letters that also do not appear in the Code of Federal Regulations, *see* Pls.' Br. at 33). And HHS did not claim *Chevron* deference.

Contrary to Plaintiffs' suggestion, *see* Pls.' Br. at 33, the agency also did not "explicitly invoke[] its general legislative authority." *Mock*, 75 F.4th at 580 (citation omitted). Though the Revised Bulletin notes that OCR "administers and enforces the HIPAA Rules," AR1, unlike the rule at issue in *Mock*, the Revised Bulletin does not "explicitly" cite any statutory rulemaking authority under HIPAA. *Id.* (agency invoked its legislative authority by citing statutes conferring rulemaking authority); *see also Factoring Criteria for Firearms with Attached "Stabilizing Braces,"* 88 Fed. Reg. 6478, 6481 (Jan. 31, 2023) (expressly citing authority for "administering and enforcing" statutes, including "provisions . . . that authorize the Attorney General to promulgate regulations"). Nor can Plaintiffs conjure an explicit reference from the Revised Bulletin's footnote citation of 45 C.F.R. part 160. *See* Pls.' Br. at 33. That footnote cites the entirety of 45 C.F.R. parts 160 and 164, *i.e.*, the HIPAA Rules. A wholesale reference to the HIPAA Rules is hardly an *explicit* invocation of HHS's rulemaking authority. Lastly, the Revised

Bulletin itself does not produce effects on private interests. Those all flow from the HIPAA Rules' preexisting requirements.

Accordingly, the Revised Bulletin is not a legislative rule and did not require notice-and-comment rulemaking.

III. ANY RELIEF SHOULD BE APPROPRIATELY TAILORED.

Plaintiffs are not entitled to relief on any of their claims. But if the Court were to conclude otherwise, it should at most enter a declaratory judgment, not the injunctive relief that Plaintiffs request. *See* Compl. at 21 (prayer for relief).

"An injunction is a drastic and extraordinary remedy, which should not be granted as a matter of course." *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 165 (2010). Where "a less drastic remedy" is "sufficient to redress [the plaintiff's] injury, no recourse to the additional and extraordinary relief of an injunction [is] warranted." *Id.* at 165–66. Here, Plaintiffs have made no attempt to show that a declaratory judgment would be insufficient to redress their injuries.

Nor have they attempted to make the traditional showing required for the extraordinary remedy of injunctive relief. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006) (identifying four factors plaintiffs must show to establish entitlement of injunctive relief). That omission alone is reason enough to withhold injunctive relief. *See Bluefield Water Ass'n, Inc. v. City of Starkville, Miss.*, 577 F.3d 250, 253 (5th Cir. 2009) (injunction "should not be granted unless the party seeking it has clearly carried the burden of persuasion on all [four] requirements"). But even if that were not the case, for the reasons explained above, the equities do not favor injunctive relief here. Plaintiffs and their members do not claim to be irreparably harmed. And in the entirely hypothetical event that OCR were to determine that any of them were out of compliance with HIPAA and initiate an enforcement action, they would have the benefit of a

lengthy administrative process followed by judicial review, which would provide them a full opportunity to raise their challenge to the HIPAA Rules' application to tracking technologies on unauthenticated webpages before facing any legal consequences for potential violations of the HIPAA Rules. On the other hand, there is substantial public interest in preventing the impermissible disclosure of PHI and the resulting loss of privacy for individuals, which itself is irreparable, tipping the balance of the equities against entering an injunction.[8]

CONCLUSION

For the foregoing reasons, the Court should deny Plaintiffs' motion for summary judgment and grant Defendants' motion for summary judgment.

Dated: March 21, 2024

Respectfully submitted,

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ERIC B. BECKENHAUER
Assistant Director
Civil Division, Federal Programs Branch

/s/ Leslie Cooper Vigen
LESLIE COOPER VIGEN
Senior Trial Counsel (D.C. Bar No. 1019782)
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, NW
Washington, DC 20005
Tel: (202) 305-0727

[8] Plaintiffs also request that the Court "set aside" the challenged portion of the Revised Bulletin. Compl. at 21. To the extent that request amounts to a request for vacatur of the challenged portion of the Revised Bulletin, Defendants recognize that the Fifth Circuit has held that vacatur is generally an appropriate remedy in an APA action, *see Data Mktg. P'ship v. U.S. Dep't of Labor*, 45 F.4th 846, 859 (5th Cir. 2022), but expressly preserve all arguments that the APA does not permit vacatur, particularly on a universal basis. *See United States v. Texas*, 143 S. Ct. 1964, 1980 (2023) (Gorsuch, J., concurring in the judgment, joined by Thomas and Barrett, JJ.) (noting that the Court has never squarely decided whether vacatur is a permissible remedy if a rule is held invalid under the APA).

Fax: (202) 616-8470
Email: leslie.vigen@usdoj.gov

Counsel for Defendants

CERTIFICATE OF SERVICE

I hereby certify that on March 21, 2024, I electronically filed this document with the Clerk of the Court for the United States District Court for the Northern District of Texas by using the CM/ECF system. Counsel in the case are registered CM/ECF users and service will be accomplished by the CM/ECF system.

/s/ Leslie Cooper Vigen